SecuMailer

Whitepaper

Sicher E-Mailen

Warum sollten Sie sich für eine E-Mail-Sicherheit entscheiden, die Ihnen im Weg steht?

Mit SecuMailer erreichen Sie Ihre Bürger sicher und mühelos.



TÜVNORD TÜV NORD Nederland B.V. ISO 27001 tuv.nl

TÜVNORD TÜV NORD Nederland B.V. NEN 7510 tuv.nl

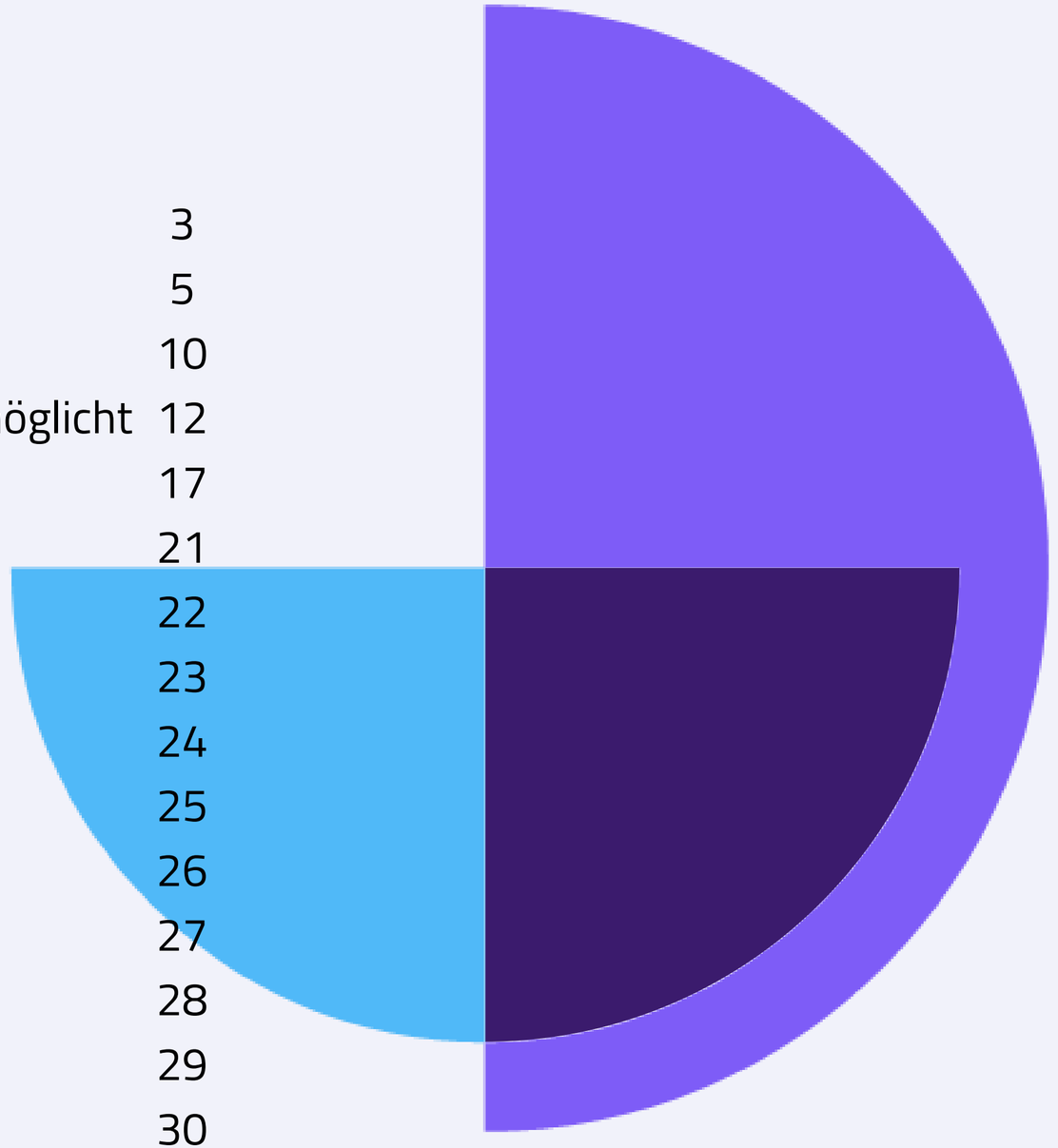
CYBERSECURITY™ MADE IN EUROPE

eIDAS

THIRD PARTY ASSURANCE REPORT ISAE 3000 SERVICE ORGANIZATIONS SOC 2 TYPE II AUDIT COMPLETED

Inhalt

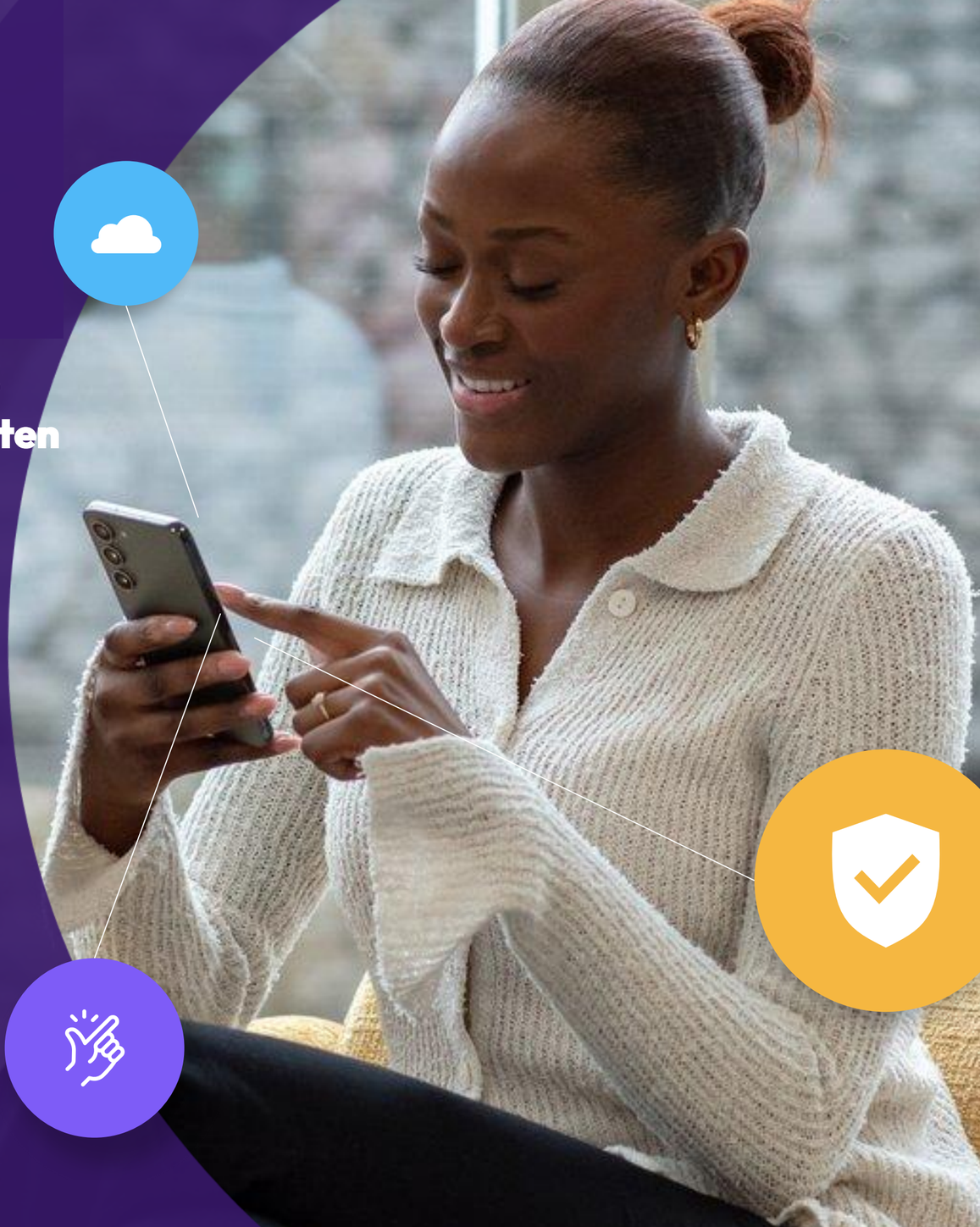
Einführung SecuMailer	3
Warum SecuMailer?	5
Vertrauliche Daten teilen: DSGVO und NIS2	10
Wie SecuMailer sicheres und benutzerfreundliches E-Mailen ermöglicht	12
Anwendungsfall Raad voor de Kinderbescherming	17
Funktionalitäten	21
Funktionen SecuMailer	22
Funktionen für Administratoren	23
Große Dateien mit SecuFiler teilen	24
Einschreiben	25
Anwendungsfall BVCM	26
Unternehmensfunktionen	27
Smart Encryption	28
Anwendungsfall GGD GHOR	29
Dutch Private Cloud: Datenhoheit in den Niederlanden	30



Mit SecuMailer können Sie sicher E-Mails versenden, ohne auf die Benutzerfreundlichkeit unsicherer E-Mails verzichten zu müssen.

Was SecuMailer einzigartig macht:

- Wir liefern den Inhalt Ihrer E-Mail sicher in den Posteingang des Empfängers
- Keine Plug-ins, sondern eine Verbindung auf Mailserver-Ebene
- Mitarbeiter versenden E-Mails, SecuMailer sorgt für die Sicherheit, als Unternehmen behalten Sie die Kontrolle
- Nie wieder unbeabsichtigte Sicherheitslücken: Jede E-Mail wird sicher versendet
- Hilft Ihnen bei der Einhaltung von DSGVO, NTA 7516, eIDAS, NIS2 und DORA
- Vollständige Datenhoheit: Ihre Daten bleiben in Europa



Einige unserer Kunden



Warum SecuMailer?

Nachweisbare Compliance und rechtsgültige E-Mail-Kommunikation

DSGVO

- Sicherer Transport: TLS 1.3, DANE, DNSSEC
- Keine Speicherung von Inhalten, Daten bleiben innerhalb der EU
- DSGVO-Konformität jährlich in der eIDAS-Konformitätsbewertung geprüft

eIDAS Qualified Registered Electronic Mail Service (QREMS)

- Rechtlicher Nachweis von Identität, Integrität und Zustellung
- Anerkennung der elektronischen Zustellung als rechtsgültige Sendung („digitale Einschreiben“)

Sicherer E-Mail-Transport

- SPF, DKIM, DMARC, Protokollierung, 2FA, TLS-Sicherheit
- Automatischer Fallback auf verschlüsseltes Portal bei unsicheren Mailservern

ISO 27001 / NEN 7510 / konform mit NTA 7516

- Für medizinische, rechtliche und behördliche Kommunikation
- Vollständiger Prüfpfad und Empfangsnachweis

Wie Smart Encryption funktioniert

Wenn eine Nachricht über SecuMailer versendet wird, wird sie zunächst über eine sichere Verbindung übertragen und anschließend mit Smart Encryption verschlüsselt, bevor sie den Posteingang des Empfängers erreicht. Die Nachricht befindet sich also verschlüsselt im Posteingang und nicht auf einem externen Portal.

Der Empfänger muss nichts installieren oder konfigurieren. Über einen sicheren Link öffnet er die Nachricht, und die Entschlüsselung erfolgt lokal im Browser. Die erforderlichen Schlüssel werden vorübergehend im Browser generiert und verlassen somit niemals die Umgebung des Empfängers.

Das bedeutet:

- Der Absender versendet sicher, ohne Zertifikatsverwaltung.
- Der Empfänger liest sicher, ohne zusätzliche Software.
- Der Inhalt bleibt verschlüsselt; die Schlüssel verlassen niemals die Umgebung des Empfängers.

Erleben Sie den Komfort gewöhnlicher E-Mails mit der Sicherheit einer End-to-End-Verschlüsselung ohne die Komplexität von S/MIME.

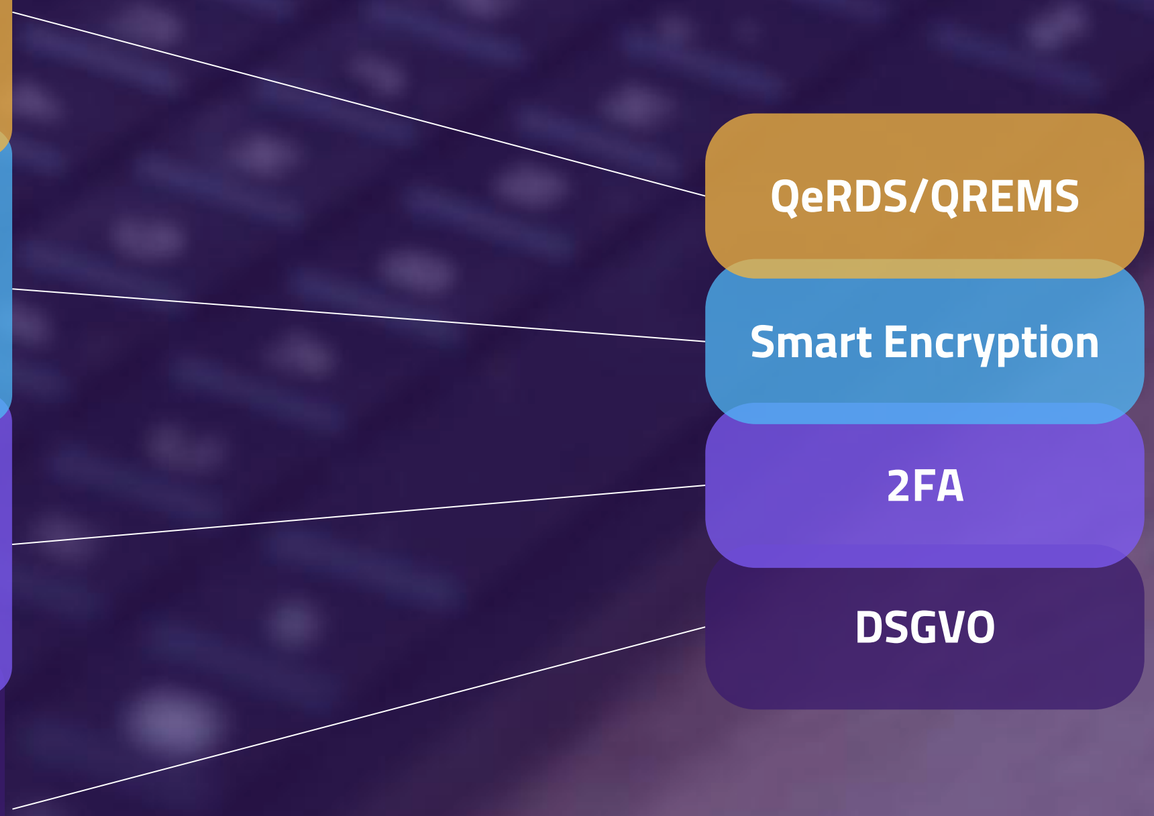
Die 4 Sicherheitsniveaus von SecuMailer

Auf der höchsten Stufe QeRDS/QREMS, die sowohl die mittlere als auch die hohe Stufe um einen zusätzlichen Zustellungsnachweis erweitert.

Auf hoher Stufe Smart Encryption: zusätzliche Verschlüsselung für streng vertrauliche Daten.

Auf der mittleren Stufe 2FA, vertrauliche Daten durch Anwendung der Zwei-Faktor-Authentifizierung des Empfängers.

Auf der Grundstufe DSGVO, nicht vertrauliche personenbezogene Daten.



Wie können Sie vertrauliche Daten sicher versenden, ohne dass dies zu Lasten der Zeit, der Benutzerfreundlichkeit oder der Aufmerksamkeit für Ihre Arbeit geht?

Es ist notwendig, vertrauliche Daten zu schützen.

Auf dem Papier klingt das gut, aber in der Praxis bedeutet es oft:

- Frust durch umständliche Codes
- Zeitaufwändige Aufgabe, die Sie von Ihrer Arbeit ablenkt
- Empfänger, die die E-Mails nicht öffnen, weil sie zu viele Schritte durchlaufen müssen

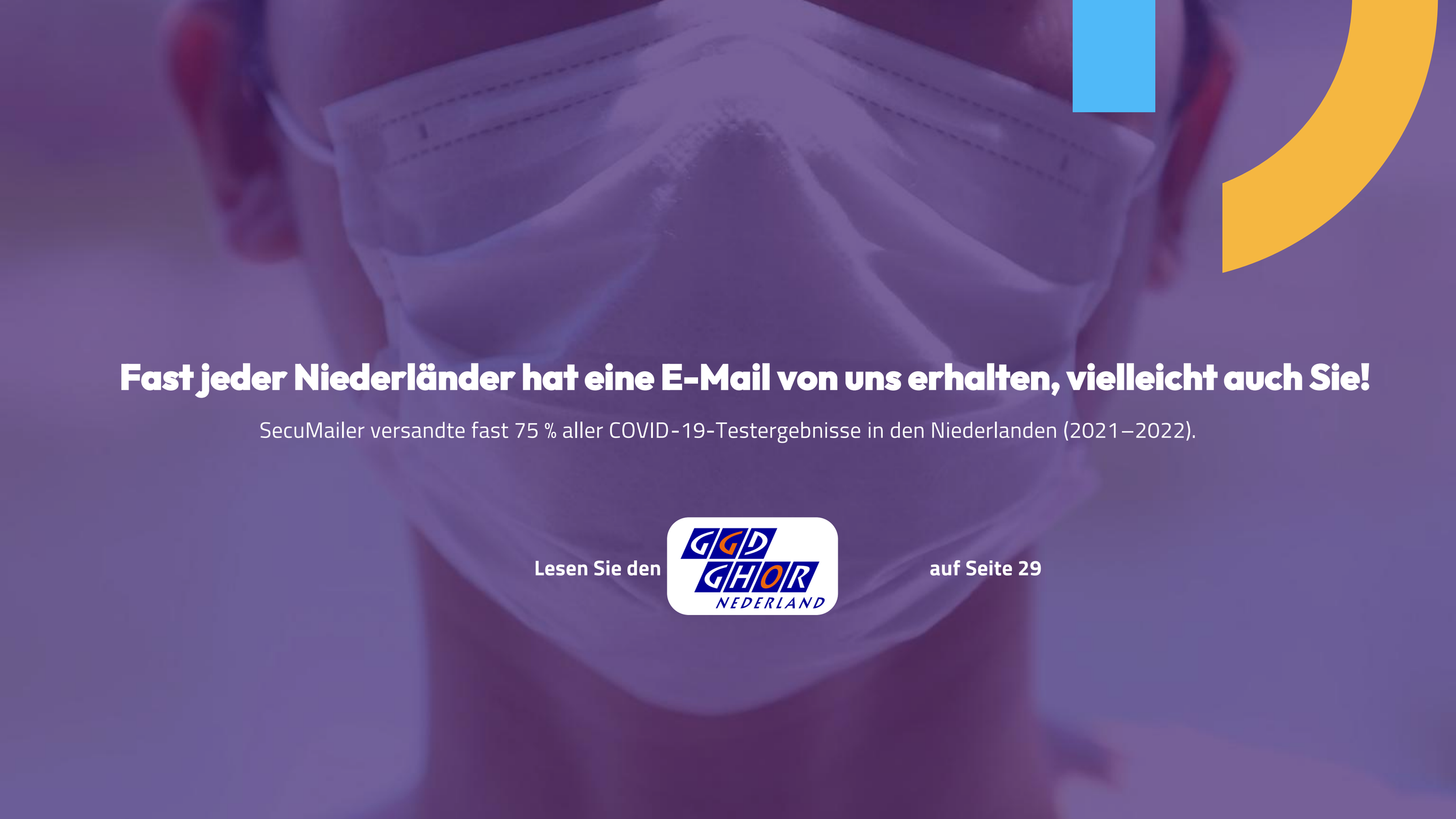
Am liebsten würde man eine normale E-Mail versenden, aber das ist nicht sicher. Der Ansatz von SecuMailer macht es möglich! Durch die zentrale Verwaltung des Sicherheitsniveaus müssen sich die Mitarbeiter keine Gedanken mehr über die E-Mail-Sicherheit machen. Keine zusätzlichen Schritte, keine Plug-ins, einfach nur E-Mails versenden.

Das Ergebnis? Mehr Zeit für die Pflege, weniger Frust, nachweislich sicher bei jeder E-Mail.



Vertrauliche Daten teilen: Hilfe bei DSGVO und NIS2

- Für vertrauliche Daten und personenbezogene Daten von Einwohnern
- 2FA mittels SMS-Code
- Die Authentifizierung bleibt maximal 90 Tage gültig, statt sich bei jeder Nachricht in ein Portal einzuloggen
- Maximal 4 SMS pro Jahr
- Interoperabilität durch Zugehörigkeit zum Interoperabilitätsnetzwerk sicherer E-Mail-Anbieter
- Die E-Mails sind immer dort, wo Sie sie erwarten: in Ihrem Postfach und im Postfach des Empfängers



Fast jeder Niederländer hat eine E-Mail von uns erhalten, vielleicht auch Sie!

SecuMailer versandte fast 75 % aller COVID-19-Testergebnisse in den Niederlanden (2021–2022).

Lesen Sie den GGD GHOR NEDERLAND auf Seite 29

Wie SecuMailer sicheres E-Mailen sicher und benutzerfreundlich macht, ohne Kompromisse einzugehen:



Beibehaltung der E-Mail-Erfahrung

Nachdem sich Ihr Empfänger authentifiziert hat, liefern wir die E-Mail in den Posteingang des Empfängers. Nach der Zustellung verschwinden die Daten von unserem Server, so wie ein Postbote eine leere Tasche hat, nachdem er den Brief in den Briefkasten geworfen hat. Als Organisation haben Sie die Kontrolle: Sie legen fest, wie lange die Authentifizierung gültig bleibt (maximal 90 Tage). In der Zwischenzeit liefern wir alle E-Mails sicher an die Empfänger und helfen Ihnen bei der Einhaltung von DSGVO, NIS2, eIDAS, ISO 27001, BIO und NTA 7516.



Hilfe bei DSGVO, NTA 7516, eIDAS, NIS2 und DORA

SecuMailer hilft Ihrem Unternehmen, die geltenden Gesetze und Vorschriften einzuhalten. Unsere Datenschutzexperten sind mit allen Einzelheiten bestens vertraut. Zusammen mit unserem Produkt helfen sie Ihnen, alle Anforderungen in Bezug auf Datenschutz und Sicherheit zu erfüllen.

Keine Einmischung von Plug-ins

SecuMailer arbeitet im Hintergrund, ohne dass Sie zusätzliche Software installieren müssen. Keine Probleme mit Updates oder Kompatibilität, einfach und effektiv! Durch eine Verbindung auf Mailserver-Ebene und den Einsatz unserer DLP (ein kleines Sprachmodell hilft, den Inhalt von E-Mails zu analysieren) ist der Verwaltungsaufwand für die IT minimal.

Wenn Sie eine aktive Benutzerunterstützung direkt in Outlook wünschen, ist auch das möglich. Verwenden Sie dazu unser webbasiertes Add-in, das den Client nicht beeinträchtigt, immer automatisch die neuesten Sicherheitsfunktionen enthält und gut mit den Windows-Updates zusammenarbeitet.





Sicherheitsstufe zentral verwaltet

Durch die Verlagerung des Sicherheitsniveaus vom Mitarbeiter zu einer zentralen Stelle in der Organisation müssen sich die Mitarbeiter nicht mehr um sicheres E-Mailen kümmern. So können sie die eingesparte Zeit für ihre Arbeit nutzen, ohne das Risiko unsicherer E-Mail-Versendung einzugehen. Als Organisation legen Sie fest, wer auf welcher Sicherheitsstufe E-Mails versendet und welche Ausnahmen gelten. Dies können Sie ganz einfach über das Verwaltungsportal einstellen. Auch unsere DLP-Lösung kann hierfür eingesetzt werden.

Datenhoheit EU

Unsere Server laufen ausschließlich innerhalb der europäischen Cloud. Mit der Dutch Private Cloud können unsere Kunden ab dem ersten Quartal 2027 die Verarbeitung in einer niederländischen privaten Cloud wählen. SecuMailer speichert keine unnötigen Daten. Sobald die E-Mail zugestellt werden kann (nach Authentifizierung des Empfängers), wird sie abgerufen und zugestellt. Dadurch ist eine Datenminimierung gewährleistet.

Cloud-Souveränität in den Niederlanden

Ab dem ersten Quartal 2027 wird SecuMailer in der privaten Cloud in den Niederlanden verfügbar sein. Unsere Kunden können dann wählen, ob sie die SaaS-Plattform in einer niederländischen privaten Cloud-Umgebung nutzen möchten. Damit ist eine vollständige Unabhängigkeit von AWS Europe möglich. Einflüsse ausländischer Gesetzgebungen wie Cloudact und „Blacklisting“ durch die US-Politik sind dann ausgeschlossen. Damit werden die Risiken für die Geschäftskontinuität stark verringert.



Raad voor de Kinderbescherming
Ministerie van Justitie en Veiligheid

Rat für Kinderschutz (Kunde seit 2023)

„Im Durchschnitt versenden wir täglich 130 geschäftliche E-Mails. Aber dies muss auch sicher geschehen.“

Vollständigen Case lesen



Die Herausforderung

Der Schutz der Privatsphäre und die Einhaltung gesetzlicher Vorschriften im Bereich der sicheren E-Mail-Kommunikation sind unverzichtbar, da viele personenbezogene Daten per E-Mail versendet werden.

Die Benutzerfreundlichkeit muss optimal sein. Es wird viel mit natürlichen Personen wie Eltern, Pflegeeltern und Erziehungsberechtigten per E-Mail kommuniziert. Die technische Integration muss einfach sein und sich in bestehende cloudbasierte Arbeitsumgebungen einfügen.

Die Lösung

Im September 2023 hat der Rat für Kinderschutz sicheres E-Mailen mit SecuMailer eingeführt.

Das Ergebnis

Durch die Beibehaltung der normalen E-Mail-Funktionalität wird eine hervorragende Benutzererfahrung ohne gemeldete Probleme erreicht.

Hilft bei der Einhaltung von Gesetzen und Vorschriften.
Sicheres E-Mailen lässt sich vollständig in cloudbasierte Arbeitsumgebungen integrieren, ohne dass ein Plug-in erforderlich ist.

Eine Lösung, beliebt bei allen Beteiligten



Benutzer

Keine Sorgen und kein Ärger mehr dank sicherem E-Mail-Versand
Der Benutzer versendet E-Mails ganz normal über seinen gewohnten E-Mail-Client, ohne zusätzliche Schritte.



IT/Administratoren

SecuMailer lässt sich nahtlos in die bestehende Arbeitsumgebung integrieren. Durch die Verknüpfung auf Mailserver-Ebene ist der Wartungsaufwand minimal. Zustellungsnachweise und Berichte sind verfügbar. Die Lösung ist so einfach, dass jeder, der E-Mails versenden kann, sie sofort ohne Schulung und ohne Hilfe der IT-Abteilung nutzen kann.

Datenschutz- & Sicherheitsbeauftragte

SecuMailer ist nach ISO 27001 und NEN 7510 zertifiziert, eIDAS-qualifiziert (QREMS), verfügt über einen ISAE 3000 SOC 2 Typ II-Bericht und das ECSO-Label und ist konform mit NTA 7516. Genau wie ein Postbote, der einen Brief zustellt und danach nichts mehr in seiner Tasche hat, liefert SecuMailer die E-Mail sicher und ohne unnötige Speicherung von Daten.



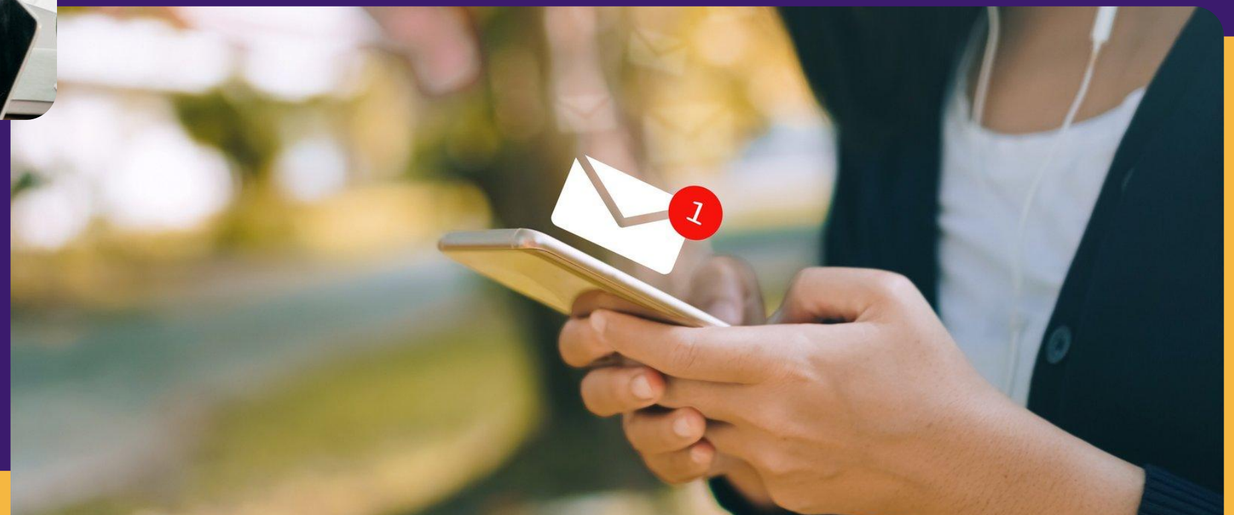
Empfänger:

Die E-Mail kommt ganz normal im Posteingang an, genau dort, wo der Empfänger sie erwartet. Die Authentifizierung ist nur einmal alle 90 Tage erforderlich (Standard), während der Empfänger in der Zwischenzeit eine normale E-Mail-Erfahrung mit dem Gesundheitsdienstleister hat.



Geschäftsführung & Einkauf:

Sie zahlen nur für das, was Sie nutzen, und sparen Wartungskosten dank geringer IT-Auslastung. Gleichzeitig minimieren Sie das Risiko von Bußgeldern oder Reputationsschäden, da das Produkt immer verfügbar ist. Dank kontinuierlicher Innovation sind Sie für die Zukunft gerüstet.



SecuMailer

VS

Alternative Lösungen

1. **Einfach per E-Mail**
   Echte E-Mails, die im Posteingang des Empfängers ankommen.
2. **Datenminimierung**
   E-Mails werden nicht gespeichert: Was nicht da ist, kann auch nicht verloren gehen.
3. **Kein Plugin**
   Alle Funktionen werden über die Standard-E-Mail-Anwendung ausgeführt.
4. **Zentral geregelte Sicherheitsrichtlinien**
   Jede E-Mail ist immer verschlüsselt und wird niemals versehentlich unsicher versendet.
5. **E-Mails von jedem Gerät und jedem E-Mail-Client**
   Unter anderem Outlook und Gmail for Business von Laptop, Smartphone und Tablet.
6. **Einfaches E-Mailen, keine Schulung erforderlich**
   Sicheres E-Mailen muss nicht kompliziert sein.
7. **Datensouveränität in der EU**
   Immer innerhalb der EU, ab dem ersten Quartal 2027 auch in der Dutch Private Cloud möglich.

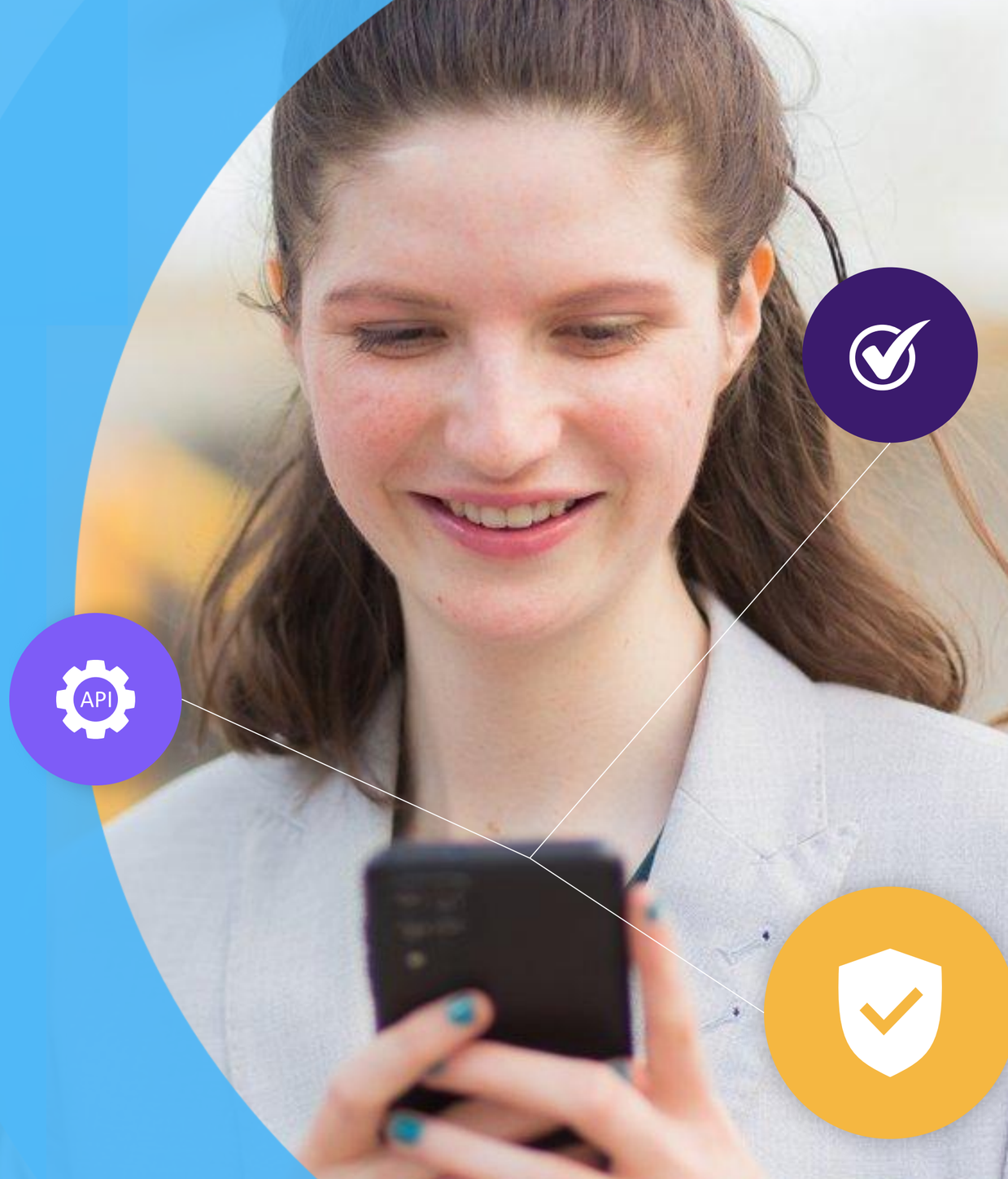
1. **Nachricht senden**
   Nachricht nur über das Portal lesbar.
2. **Datenkonzentration**
   Alle E-Mails werden an einem Ort gespeichert, was ein großes Risiko darstellt.
3. **Plug-in erforderlich**
   Die Verwendung eines Plug-ins hat Auswirkungen auf die IT, den Arbeitsplatz und den
4. **Die Wahl der Sicherheitsmaßnahmen liegt beim Absender**
   Erhöhtes Risiko menschlicher Fehler.
5. **Nur Outlook wird unterstützt**
   Aufgrund der Abhängigkeit vom Plug-in.
6. **Zusätzlicher Aufwand für den Absender**
   Angepasste Vorgehensweise (keine echte E-Mail-Erfahrung).
7. **Keine Datenhoheit**
   Eigentum oder enge Verflechtung mit amerikanischen Parteien.


Funktionalitäten

Funktionalitäten von SecuMailer

Welche Funktionen sind verfügbar?

- **Standardverschlüsselung:** Alle E-Mails werden standardmäßig verschlüsselt versendet.
- **Digitale Signatur:** SecuMailer versieht jede E-Mail mit einer digitalen Signatur.
- **Empfangsbestätigung:** SecuMailer protokolliert, wer eine Nachricht wann versendet und empfangen hat.
- **Authentifizierung:** Möglichkeit, 2FA für bestimmte E-Mails oder Benutzer zu erzwingen.
- **DLP und Geschäftsregeln:** Möglichkeit, Regeln für die automatische Anwendung von Sicherheitsmaßnahmen basierend auf dem Inhalt der E-Mail festzulegen.
- **API-Anbindungen:** Anbindungen an verschiedene Systeme wie CRM, EPD und ERP.





Admin-Funktionen

- **Verwaltungsportal:** Zugang zu einem Portal mit folgenden **Funktionen:** Einblick in den E-Mail-Verkehr (Events).
- Verwaltung von Konten und Telefonnummern (Accounts).
- Festlegen der Mailbox-Einstellungen pro Domain (Mailbox Settings).
- **Anpassen von Benachrichtigungen (Branding).**
- **Berichtsfunktionen:** Möglichkeit zur Erstellung von Berichten über versendete E-Mails und Sicherheitsvorfälle.
- **Support:** Zugriff auf Online-Handbücher, technische Dokumentation und ein Support-Team.

Große Dateien mit SecuFiler sicher teilen

Mit SecuFiler können Sie große Dateien sicher bis zu einer Größe von 5 TB über das Outlook-Add-in oder die SecuFiler-Webanwendung teilen.

- **Teilen über den Browser:** Integrieren Sie SecuFiler als Seite in die Website Ihrer Organisation. Über diese Seite können Ihre Kunden alle vertraulichen Dokumente einfach und sicher an Ihre Organisation senden.
- **Breite Palette an Dateitypen wie .pdf, .jpg, .png und .mp4**
- **Geeignet für medizinische Informationen:** Dank der Möglichkeit, 2FA anzuwenden, versenden Sie große Dateien gemäß den Richtlinien der NTA 7516.





Einschreiben per E-Mail

Versenden Sie eine registrierte E-Mail mit dem gleichen rechtlichen Status wie ein Einschreiben. SecuMailer ist hierfür eIDAS-qualifiziert.

- SecuMailer ist eIDAS-qualifiziert für den Qualified Registered Electronic Mail Service (QREMS) und steht auf der EU-Vertrauensliste.
- **Qualifizierte E-Mail:** Eine qualifizierte E-Mail hat Rechtsstatus und kann als rechtsgültiges Beweismittel verwendet werden.
- **Einfach registriert (Versandnachweis):** Möglichkeit, einen Zustellnachweis für versendete E-Mails anzufordern.



BVCM ist Kunde seit 2022

„Wir haben mit drei Anbietern gesprochen, die eine ähnliche Lösung angeboten haben, aber SecuMailer hat sich deutlich von den anderen abgehoben.“

[Vollständigen Case lesen]

Die Herausforderung

BVCM versendet täglich sensible Informationen an Kunden, Schuldner und Gerichte. Als sich die Gesetzgebung änderte, wurde sicherer E-Mail-Versand zu einer Notwendigkeit. Für BVCM stand fest: Es muss für die Mitarbeiter praktikabel bleiben, ohne zusätzlichen Aufwand oder unnötige Tools.
Kunden verlassen sich darauf, dass Vereinbarungen eingehalten werden und die Kommunikation mit Schuldnern tatsächlich stattfindet. Dies erforderte eine Lösung, die nicht nur die Sicherheit gewährleistet, sondern auch Einblick in eventuelle Zustellprobleme gibt.

Die Lösung

Im Jahr 2025 hat BVCM die qualifizierte registrierte E-Mail (QREMS) in sein Inkasso-Backend-System integriert.

Das Ergebnis

Mit SecuMailer spart BVCM Zeit, Geld und Sorgen. Die E-Mails sind nachweislich sicher und rechtsgültig, ohne Aufwand für Mitarbeiter oder Empfänger. Auch der Versand von Einschreiben erfolgt nun effizient über eIDAS-Mail. Die Mitarbeiter können sich auf ihre eigentliche Arbeit konzentrieren, während die E-Mail-Sicherheit im Hintergrund funktioniert.

Corporate Funktionen

- **REST-API-Verbindungen:** Verbindungen zu verschiedenen Backoffice-Systemen.
- **Mailmerge:** Möglichkeit zum Versenden personalisierter Massen-E-Mails.
- **SAML:** Single Sign-On (SSO)-Funktionalität für den Zugriff auf das Verwaltungsportal.
- **SIEM/SOC RBAC:** Möglichkeit zur Integration mit Security Information and Event Management (SIEM) und Security Orchestration, Automation and Response (SOAR) Systemen.
- **Eigenes Corporate Design: Anpassung des Corporate Designs von Benachrichtigungen und der Weboberfläche.**





Smart Encryption

- **Immer verschlüsselt:** Der Inhalt ist vom Versand bis zum Empfang vollständig verschlüsselt, sogar im Postfach des Empfängers.
- Authentifizierung über DigiD, SMS oder andere ID-Methoden möglich
- Volle Kontrolle über die Informationen durch den Absender: Die Nachricht ist sowohl während des Transports als auch in der E-Mail beim Empfänger immer verschlüsselt.
- **Geeignet für eigenes DLP:** Der Absender sendet eine gesicherte E-Mail über eine verschlüsselte Verbindung an die SecuMailer-Plattform, wo Smart Encryption angewendet wird. Dadurch hat die sendende Organisation die vollständige Kontrolle und Übersicht darüber, welche Informationen die Organisation verlassen dürfen.
- **Erweiterte Browser-Entschlüsselung:** Die vollständige Entschlüsselung erfolgt lokal im Speicher des Browsers. Dadurch ist keine Sammlung von Zertifikaten beim Empfänger erforderlich, was Smart Encryption besonders für Einwohner und Patienten geeignet macht.
- **Zertifizierung: ISO 27001, eIDAS QeRDS/QREMS, konform mit NTA 7516 und DSGVO.**



GGD-GHOR ist seit 2021 Kunde

“Bis zu 1 Million E-Mails pro Tag sicher versendet während der Corona-Pandemie”

Vollständigen Case lesen

Die Herausforderung

- Schnelle Skalierbarkeit, um bis zu 1 Million E-Mails pro Tag sicher versenden zu können
- Optimale Benutzerfreundlichkeit. E-Mails werden vor allem an Bürger verschickt.
- Medizinische Daten müssen unter Einhaltung der europäischen Gesetze und Vorschriften per E-Mail versendet werden können.

Die Lösung

Seit 2021 nutzt GGD GHOR die Mail-Merge-Lösung von SecuMailer, um mehr als 50 Millionen E-Mails mit medizinischen Informationen an Bürger zu versenden.

Das Ergebnis

- Keine Datenlecks
- Keine Sicherheitsvorfälle
- Keine Auswirkungen auf den Service Desk

Finanziert durch die Europäische Union

Dutch Private Cloud

Vollständige Datenhoheit: Ab dem ersten Quartal 2027 kann Ihr Unternehmen die Verarbeitung sicherer E-Mails, einschließlich der temporären Speicherung (erforderlich, wenn sich der Empfänger noch authentifizieren muss), vollständig in einer niederländischen privaten Cloud stattfinden lassen.

Europäische Lösung: Die Dutch Private Cloud gibt Ihrem Unternehmen die Gewissheit, dass Ihre Daten für sicheres E-Mail-Versenden unter europäischer Aufsicht stehen und in den Niederlanden gehostet werden, unterstützt durch das ECSO-Label und entwickelt mit Hilfe des EFRO-Programms.

Datenminimierung als Ausgangspunkt: Nachrichten und Anhänge werden sofort nach der Zustellung gelöscht. Die E-Mail-Nachricht, die vor der Zustellung vorübergehend gespeichert wird, befindet sich mit der Dutch Private Cloud sicher in den Niederlanden.



Entwickelt mit EU-Förderung aus Kansen voor West 3.



SecuMailer sehen? Vereinbaren Sie eine Demo!

Kontaktieren Sie uns:

www.secumailer.de

info@secumailer.com

+31 320 337 381

Oder vereinbaren Sie direkt online einen Termin:

Unverbindliche Demo vereinbaren

